Target

Per questa simulazione, il target scelto sarà `example.com`, un dominio utilizzato comunemente come esempio nei documenti.

Strumenti Utilizzati

1. **Google (Google Hacking)**
2. **Dmitry**
3. **Recon-ng**
4. **Maltego**

---

1. Utilizzo di Google Hacking

Query Utilizzate:

- **Ricerca di Pagine di Login:**

  ```
  plaintext
  site:example.com inurl:login
  ```

  Risultati: Trovate diverse pagine di login, ad esempio `example.com/login.php`.

- **Ricerca di File Sensibili:**

  ```
  plaintext
  site:example.com filetype:pdf
  ```

  Risultati: Trovati alcuni file PDF, ad esempio `example.com/files/document1.pdf`.

- **Ricerca di Pagine di Amministrazione:**

  ```
  plaintext
  site:example.com inurl:admin
  ```

  Risultati: Trovate pagine di amministrazione, ad esempio `example.com/admin`.

- **Ricerca di Directory Aperte:**

  ```
  plaintext
  site:example.com intitle:"index of"
  ```

  Risultati: Trovate directory aperte, ad esempio `example.com/files/`.

2. Utilizzo di Dmitry

Comandi Utilizzati:

- **Raccolta Informazioni di Base:**

```
bash
dmitry -win example.com
```

Risultati:

- Whois Information
- Indirizzi IP associati al dominio
- Hostname

- **Ricerca di Sottodomini e Email:**

```
bash
dmitry -s -e example.com
```

Risultati:

- Sottodomini: `sub.example.com`
- Email: `info@example.com`

3. Utilizzo di Recon-ng

Moduli Utilizzati:

- **Raccolta di Informazioni di Base:**

```
bash
recon-ng
workspaces create example_workspace
modules load recon/domains-hosts/whois_pocs
set source example.com
run
```

Risultati: Informazioni whois e contatti associati al dominio.

- **Ricerca di Sottodomini:**

```
bash
modules load recon/domains-hosts/bing_domain_web
set source example.com
run
```

Risultati: Sottodomini trovati.

- **Raccolta di Indirizzi IP:**

```
bash
modules load recon/hosts-hosts/resolve
set source example.com
run
```

Risultati: Indirizzi IP associati ai domini.

4. Utilizzo di Maltego

Passaggi Eseguiti:

- **Creazione di un Nuovo Grafico:**
  - Inserito il dominio `example.com`.
- **Utilizzo di Trasformazioni per la Raccolta di Informazioni:**
  - **To IP Address [DNS]**: Identificati indirizzi IP associati.
  - **To Domain [DNS]**: Trovati sottodomini.
  - **To Email Address [Email Search]**: Trovati indirizzi email associati al dominio.

Risultati:

- Grafico visivo che mostra la relazione tra il dominio principale, i sottodomini, gli indirizzi IP e gli indirizzi email.

Report Finale

1. Google Hacking

- **Target:** example.com
- **Query Utilizzate:**
  - `site:example.com inurl:login`
  - `site:example.com filetype:pdf`
  - `site:example.com inurl:admin`
  - `site:example.com intitle:"index of"`
- **Risultati:** Pagine di login, file PDF sensibili, pagine di amministrazione, directory aperte.

2. Dmitry

- **Target:** example.com
- **Comandi Utilizzati:**
  - `dmitry -win example.com`
  - `dmitry -s -e example.com`
- **Risultati:** Informazioni Whois, indirizzi IP, sottodomini, email.

3. Recon-ng

- **Target:** example.com
- **Moduli Utilizzati:**
  - `recon/domains-hosts/whois_pocs`
  - `recon/domains-hosts/bing_domain_web`
  - `recon/hosts-hosts/resolve`
- **Risultati:** Informazioni whois, contatti, sottodomini, indirizzi IP.

4. Maltego

- **Target:** example.com
- **Trasformazioni Utilizzate:**
  - **To IP Address [DNS]**
  - **To Domain [DNS]**
  - **To Email Address [Email Search]**
- **Risultati:** Grafico visivo con domini, sottodomini, indirizzi IP, email.

Conclusione

Questa simulazione ha dimostrato come utilizzare diversi strumenti di raccolta informazioni per ottenere dettagli importanti su un target. Le informazioni raccolte possono essere utilizzate per valutare la sicurezza del sito e prendere misure necessarie per proteggere le informazioni sensibili.